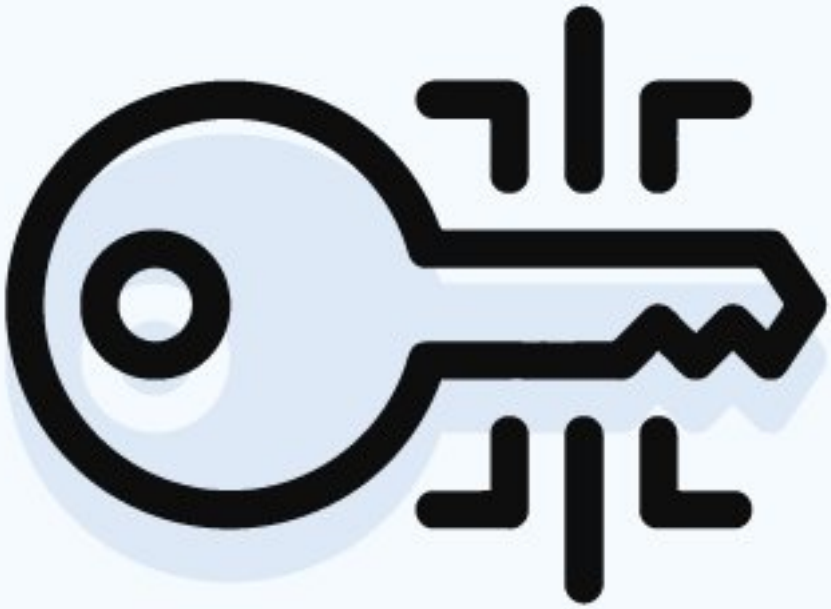

Roundtable on Encryption

September 29th, 2020

sflc.in

Roundtable on Encryption

3rd September, 2020 --- 5:00 PM IST – 7:00 PM IST

Roundtable Report

On September 3rd, 2020, Software Freedom Law Centre, India (SFLC.in) organized a multi-stakeholder round-table discussion to "Individual Liberty vs. National Security" debate, and to address the concerns arising from conflicting encryption regulations across the world through the lens of members of civil society, journalists, technologists and lawmakers. This round-table was a part of SFLC.in's on-going project on encryption.

The round-table was divided into two rounds:

Round 1: Individual Liberty vs. National Security vis-a-vis Encryption Debate

A draft National Policy on Encryption under Section 84A of the Information Technology Act, 2000 was published in2015. It was, however, withdrawn a few weeks later because it was deemed to be unfeasible, vague and problematic with respect to the usage of encryption technologies. The Government of India in its draft Intermediary Guidelines, 2018 has introduced a provision of traceability which if notified could lead to various security and privacy concerns. Globally, we are seeing a trend by governments to weaken encryption by proposing introduction of backdoors in encryption services offered by various organizations.

The objective of Round 1 was to find out if there is a way to balance the concepts of liberty and national security, while also aiming to arrive at a meaningful answer to this debate.

Round 2: Addressing Conflicting Regulations on Encryption at International Level

While encryption has enabled the exercise of right to privacy and free speech, the legal situation on encryption varies across the world. Several countries have general laws on encryption, a few of them

have restricted rights to encryption. For example: Senegal has a law on cryptography which has set maximum key size at 128 bits and use of greater key length requires authorization. Similarly, Israel regulates use of encryption through its Encryption Order. India, on the other hand, has sectoral regulations on encryption like the unified license for telecoms which does not allow bulk encryption and the RBI's regulations on Internet Banking amongst various other regulations The terms of service for internet service providers (ISPs) require 40 bit encryption. However, most companies doing business in India have moved to international standards on encryption. Through this round, we intend to find out if there is a way to harmonize various conflicting regulations on encryption across the world while adhering to human rights principles.

The conversation was under the Chatham House Rules. Nothing in this report has been attributed to any individual, institution, or affiliation, nor does it necessarily reflect SFLC.in's or any other participant's positions.

About SFLC.in

SFLC.IN is the first Indian legal services organization that works exclusively on technology, law, and policy. As a not-for-profit organization engaged in the empowerment of Indian citizens about their digital freedom and rights, it operates as a collective bringing together different stakeholders to a common platform to further the cause of digital rights. SFLC.in promotes innovation and open access to knowledge by helping policy makers make informed and just decisions regarding the use and adoption of technology. As of 2020 SFLC.in is the only Indian organization to be inducted as a member of the IFEX, a global network to defend the right to freedom of expression and information.

Table of Contents

1. Introduction

The discussions began with a round up of all the developments that had taken place in the digital ecosystem in India - the introduction of the Aadhaar card by the UIDAI, recognition of the right to privacy in the Puttaswamy judgment, the Personal Data Protection Bill (which has within it elements of non-personal data protection as well) and the contentious traceability provision in the draft Intermediary Guidelines, 2018. There was a brief discussion on the recommendation of the Ad-hoc Committee on Child Pornography. . The participants agreed that these issues cannot be viewed in isolation and need to be looked into from the perspective of global scenario, the draft data protection legislation, draft intermediary guidelines etc.This highlighted the conflict between individual liberty and national security; data protection and technological innovation etc. It is important to address the concerns raised by law enforcement agencies, this must lead to over-regulation and throttling of free speech as well as right to privacy. For instance, backdoor solutions may help the law enforcement agencies, have the potential of risking the data of those innocent or not connected with the crime in question might be exposed. The roundtable aimed to look for both technological and non-technological solutions for these issues.

2. Discussion in Round I

Impacts of complexities of technology on national security

One of the consequences of the sudden technological advancements over the years is the improvement in encryption mechanisms. This has resulted in law enforcement agencies finding it difficult to break strong modes of encryption and preventing them from conducting investigations into serious crimes, such as act terrorism. The debate around the illegality of the creation of back-doors began in India when the issue of Research in Motion (RIM) locating servers in India giving into the pressure of the Government to provide access to encrypted messages on Blackberry phones came into light. . States are now trying to come up with new methods to break encryption, while keeping pace with increasing complex technology. In last

couple of years, Australia and United Kingdom, both are parts of the "five-eyes alliance" have enacted legislations which have the potential to weaken encryption. Prior to regulating technology, we must try to first understand the complexities of encryption mechanisms. The laws then have to be synchronized with updates in technology in order to be effective.

Fundamental rights vis-a-vis encryption

The process of weakening encryption affects the right to privacy as well as free speech. On the other hand, strong encryption is an impediment to investigative capabilities of law enforcement agencies. The Government has to take into account these nuances while regulating encryption. India tried its hand at regulating encryption via the draft Encryption Policy, 2015. The Policy, however, was withdrawn because of lack of transparency, vague provisions and lack of procedural safeguards.

Similarly, the traceability provision introduced in the draft Intermediary Guidelines,2018 has also become a topic of controversy due to potential of having a chilling effect on fundamental right to privacy and free speech. While the fundamental right to privacy is not absolute in nature, it is important to ensure that blatant infringement of privacy must not be allowed in the name of protecting national security. One cannot be allowed to weaken the system at the expense of another's rights. The Puttaswamy tests provide for the procedure and the reasoning on the basis of which the right can be limited - it allows for a least intrusive mechanism for restricting privacy rights.

Debate around end-to-end encryption

It is important to remember that individual liberty and national security are not diametrically opposite each other. End-to-end encryption has served the national security concerns of different nations. However, with the rise in the use of surveillance mechanisms, it becomes important to save these little islands of privacy. It emerges as a refuge for privacy, both for the State and private players. Despite being owned by Facebook, a known privacy violator, WhatsApp provides for end-to-end encryption. When it comes to the legitimate concerns of

law enforcement agencies, gaining access to meta-data can help in finding the originator of messages. This is particularly important for crimes like child pornography and fake news. This leads to two axes of interrogation - what is technically and legally allowed when it comes to resolving these types of cases? The primary question, however, is - what should be allowed? The Blackberry model is similar to the model that Prof. Kamakoti suggested in the WhatsApp case. This, however, can lead to the problem of there being a single point of vulnerability. Unlike the US (where there are many challenges against the Patriot Act), there has been little to no litigation in India on these matters. It is thus difficult to challenge this overreach of the State.

Solutions attempted by encryption agencies

The fact that 85% of the internet is encrypted is proof of the fact that there has been a vast acceptance of the idea that encryption is a safer and preferred option for the users of the internet. Traceability has to be looked at from the purview of its impact on governance and its juxtaposition of the fundamental right to privacy. Strategically, this has to be the option we choose over the complete abdication of end-to-end encryption. This will help in addressing legitimate concerns of both parties i.e. the law enforcement agencies and the citizens. These are pertinent questions that we have to find solutions for soon, because of the increasing scenarios of hacking of phones by using bugs, spywares or other illegal means. We need to lay down checks and balances for these situations so that it becomes a more transparent process. Post the Snowden revelations, this debates has become more important, and has to be fast-tracked keeping in mind the constantly innovative nature of technology.

3. Discussion in Round II

Resolution of Human Rights Council on Encryption, 2017

In 2017, the Human Rights Council recognizing the importance of encryption to freedom of expression, privacy and related human rights, adopted a resolution encouraging *"business enterprises to work towards enabling technical solutions to secure and protect the*

confidentiality of digital communications, which may include measures for encryption and anonymity."

David Kaye's (UN Special Rapporteur on Freedom of Expression), Seminal Report on Encryption

The Rapporteur highlights the taxonomy of threats that are inconsistent with international standards of necessity, proportionality, and legitimacy— in the form of state practices, examples and concerns. This includes concerns around the ban on use of encryption, data localization laws, key-escrow laws, laws that require licensing or registration requirements, prohibition on tools designated to prohibit anonymity.

Focus on Brazil

In Brazil, this started with two constitutional claims before the Federal Supreme Court. The case was on if it is constitutional to block an application for not complying with a court order to hand over users' information. Facebook argued that it is technically incapable of handing over data since WhatsApp uses end-to-end encryption, making it impossible for the company to access the contents of a message.

Upon receiving a negative response from WhatsApp, the judges decided to block the application. In one of the articles, the standard requires the data controller to make the data available after the court decision. The Court's decision should decide on the constitutionality of the court's decisions to prevent the application from functioning temporarily due to the refusal to deliver information of users investigated for various crimes.

Article 10 of the (Fake News) Bill in Brazil compels private messaging applications to retain, for three months the chain of all communications that have been "massively forwarded". The retained data should include users who mass-forwarded the message, date and time of forwarding, and the total number of users who received the message. The traceability debate has mostly focused on malicious coordinated action on WhatsApp, which is the most popular

encrypted messaging tool in Brazil. There has been minimal discussion on the impact of other tools and services such as Telegram, Signal or iMessage.

The Metadata Retention Test

There is hope that the alternative proposals in the Fake News Bill will eliminate the traceability mandate. Alternatively, metadata retention of certain accounts for a specific period could be used by law enforcement agencies for interception of communication. Even this would require certain procedural safeguards including a court order and other standards for accessing it.

The fear is that if traceability is approved in India or Brazil, it will influence the approval of such mandate in other countries. Both countries have a soft power to influence policy in other developing countries.

The metadata retention mandate will easily pass legal/ constitutional tests in India as well. Section 67C of the Information Technology Act, 2000 already allows for such retention but has not been used in that way yet.

Worldwide trend of undermining encryption

Strong encryption is being undermined worldwide. We are seeing this in India with the draft Intermediary Guidelines, it is also happening in United States with the EARN IT Act, in Brazil as well. United Kingdom and Australia have already passed laws which undermine encryption.The technical consensus is that there is no way to provide third party access to encrypted messages. As countries consider the ways to undermine encryption, they must consider three things:

i. the impact on their economy;

ii. the impact on the security of their citizens; and

iii. the impact on their national security.

Encryption Legislation in Australia

We have already witnessed the negative impact of laws undermining encryption on the tech industry and on the economy in the United Kingdom and Australia. The Australian government passed their own encryption law (the Assistance and Access Act) in 2018, a law that basically allows the Government to have power to force companies to put in encryption back-doors. A year later, we saw in the survey of tech companies that 40% of them said that they had lost sales directly as a result of this encryption law. One thing to know is that, it has been two years since this law in Australia has been passed, and they actually have not used the power yet to weaken the encryption of a company in their country.

Just having that law in the books, and the ability to do that, caused enough mistrust of Australian tech companies that users and consumers looking for services and products, did not opt for Australian companies.

Security aspect of end-to-end encryption

Not having strong encryption puts citizens at a security risk, particularly vulnerable groups like journalists and marginalized communities. This is of particular concern now with COVID-19 as the health information requires to be secured.

End-to-end encryption is important for national security as well because it is important to keep Government communications secure. In USA, the army often uses Signal for official communications. In India, several sensitive communications by government officials as well as lawmakers happen over WhatsApp.

Overall, we need to think about security of the state and citizens, and the economy and should not have a patchwork of laws that weaken encryption. Countries need to think about laws and policies that:

i. Help in building a stronger market for encryption through procurement policies;

ii. Ensure that Governments use strong encryption for their own services; and

iii. Aims for capacity building leading to a strong cyber security industry in the country.

iv. Create public awareness on using encryption.

Observations on Encryption

The Government needs to delve into several questions before proposing any framework which weakens encryption including framing of issues surround encryption which look at it from a user-centric point of view i.e. respecting user's fundamental right to privacy, speech and expression, protection of minorties vis-a-vis national security concerns. It is important to consider the cost of diluting encryption from the perspective of businesses.

One of the examples, where following the lead is always not the best way is, the USA, UK, Australia asking Facebook not to introduce end-to-end encryption. That move was followed by Germany later and then we saw some something similar in India too.

There is a trade-off where intermediaries, in order to protect their safe harbour, may have to dilute encryption. The government requires to look at the larger conversation by all the stakeholders around the world.

The government also needs introspectively analyse whether it is a good faith actor and if people have enough trust on the government with respect to privacy especially in the backdrop of the Pegasus spyware, with the sale of Vahan database, the Personal Data Protection Bill or the Non Personal Data Governance Framework. In all these cases, privacy is seen as a subset of larger economic value data can bring in.

The best way to go forward is to see more transparent debates and consultation before and after any policy like this is brought in.

Impact of Traceability on WhatsApp's Infrastructure

WhatsApp and Facebook have been maintaining that if they are forced to break end-to-end encryption in India, they will have to do it around the world. It is a design imposition that will be

implementable at a global level. This is why they have been saying that on the basis of one jurisdiction, they cannot make changes in their platform architecture for 190+ countries.

Signal has been moving in the other direction i.e. away from traceability. As a privacy preserving open source organization, the emphasis of Signal remains in that direction. Signal's stand is very clear with respect to Australian law wherein they have clearly stated that they cannot comply with Australian encryption law even if they wanted to.

Uniformity in Encryption Policies Across Different Jurisdictions

It is unfeasible to achieve uniformity in encryption policies. What can be ensured is that the policies on encryption are positive rather than negative and they add incentives to improve security rather than incentivising poor security. Otherwise, you have a patchwork of laws which impacts businesses.

Impact of Traceability Provision on Journalists and Confidentiality of Sources

Over the last couple of years, many organizations have been having these workshops to ensure secure communication. Many of the journalists rely on WhatsApp and Signal for secure communications and there is a lingering fear given that action have been taken against media houses and journalists in the past. In the event the encryption is compromised, it will come at a huge cost to journalists.

Appendix I: Recommended Readings

1. The Draft Intermediary Guidelines, 2018

2. Australia's 2018 Assistance and Access Bill

3. The USA's EARN IT Bill

4. https://signal.org/blog/sealed-sender/

5. https://signal.org/blog/signal-private-group-system/

6. https://www.globalencryption.org/

7. https://www.medianama.com/2020/01/223-rajya-sabha-recommendations-child-porn/

8.https://signal.org/blog/earn-it/

9.https://signal.org/blog/setback-in-the-outback/

10. https://www.geant.org/News_and_Events/CONNECT/Documents/CONNECT_31.pdf

11.https://www.medianama.com/2020/06/223-encryption-misinformation/